

Compound Multiple Access Channel with Confidential Messages

Hassan Zivari-Fard^{†,††}, Bahareh Akhbari^{††}, Mahmoud Ahmadian-Attari^{††}, Mohammad Reza Aref[†]

[†]Information Systems and Security Lab (ISSL), Sharif University of Technology, Tehran, Iran

Email: hassan_zivari@ee.kntu.ac.ir, aref@sharif.edu

^{††}Department of ECE, K. N. Toosi University of Technology, Tehran, Iran

Email: {akhbari, mahmoud}@eetd.kntu.ac.ir

¹ **Abstract**—In this paper, we study the problem of secret communication over a Compound Multiple Access Channel (MAC). In this channel, we assume that one of the transmitted messages is confidential that is only decoded by its corresponding receiver and kept secret from the other receiver. For this proposed setting (compound MAC with confidential messages), we derive general inner and outer bounds on the secrecy capacity region. Also, as examples, we investigate 'Less noisy' and 'Gaussian' versions of this channel, and extend the results of the discrete memoryless version to these cases. Moreover, providing numerical examples for the Gaussian case, we illustrate the comparison between achievable rate regions of compound MAC and compound MAC with confidential messages.

I. INTRODUCTION

The wire-tap channel was first introduced by Wyner in 1975 [1]. His model consisted of a transmitter, a receiver and an eavesdropper. In the Wyner model, the eavesdropper channel was a degraded version of the legitimate receiver channel. Csiszár and Körner extended the wire-tap channel to a more generalized model called the broadcast channel with confidential message [2]. More recently, sending a confidential message over multiple-user channels have been studied under various different models [3]–[8]. We also refer the reader to [9] for a recent survey of the research progress in this area. The discrete memoryless compound Multiple Access Channel (MAC), Gaussian compound MAC with a common message and conferencing decoders, and also the compound MAC when both encoders and decoders cooperate via conferencing links were considered in [10].

In [3] the authors studied the effect of users' cooperation in multiple access channel when transmitting a confidential message. There, active cooperation between two trusted users is attained through a generalized feedback channel. In [4] a discrete memoryless multiple access channel with confidential messages was studied where each user uses the output of generalized feedback to eavesdrop the other user's private message. Ekrem and Ulukus derived n -letter inner and outer bounds for the multiple access wire-tap channel with no common message [5]. In [7], the authors studied this model assuming that there exists a common message and that the eavesdropper is unable to decode it. They also derived a rate region under the strong secrecy criterion.

In this paper, we consider Compound Multiple Access Channel with Confidential Messages (CMAC-CM). Actually, in wireless networks, there may be a scenario in which some of the users have confidential information that wish to be

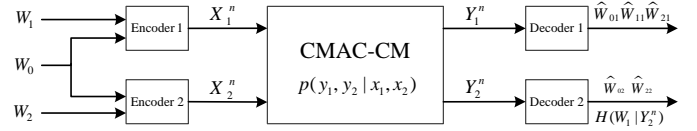


Fig. 1 Compound Multiple Access Channel with Confidential Messages (CMAC-CM)

kept secret from illegal users. In fact, in terms of information the users can be divided into legitimate and illegal users. Legitimate users are allowed to decode *all* the transmitted information (including common and private messages of all the transmitters), while illegal users are allowed to decode only the messages of their intended transmitters. Motivated by this scenario, we consider CMAC-CM as a building block of this setting. In this model, while each of the transmitters sends its own private message, both of them have a common message. One of the transmitters' private message (W_1) is confidential and only decoded by the first receiver and kept secret from the second receiver. The common message W_0 and private message W_2 are decoded by both receivers (see Fig. 1). For this model we derive single letter inner and outer bounds on the secrecy capacity region. We also consider two examples for this channel: Less noisy and Gaussian CMAC-CM.

This paper is organized as follows. In Section II, the system model is described. In Section III, an outer bound on the secrecy capacity region of CMAC-CM and also an achievable secrecy rate region for CMAC-CM are derived. Two examples are given in Section IV. The paper is concluded in Section V.

II. SYSTEM MODEL

Consider a discrete memoryless CMAC-CM with four-terminals as shown in Fig. 1. The finite sets $\mathcal{X}_1, \mathcal{X}_2, \mathcal{Y}_1, \mathcal{Y}_2$ and the transition probability distribution $p(y_1, y_2 | x_1, x_2)$ are the constitutive components of this channel. Here, X_1 and X_2 are the channel inputs from the transmitters. Also Y_1 and Y_2 are the channel outputs at the receiver 1 and receiver 2, respectively. Throughout this paper, the random variables are denoted by capital letters e.g., X, Y , and their realizations by lower case letters e.g., x, y . The set of ε -strongly jointly typical sequences of length n , on joint distribution $p(x, y)$ is denoted by $A_\varepsilon^n(P_{X,Y})$. We use X_i^n to indicate vector $(X_{i,1}, X_{i,2}, \dots, X_{i,n})$, and $X_{i,j}^k$ to indicate vector $(X_{i,j}, X_{i,j+1}, \dots, X_{i,k})$. Before discussing the achievability rate, we first define a code for the channel as follows.

Definition 1: A $(M_0, M_1, M_2, n, P_e^n)$ code for the CMAC-CM (Fig. 1) consists of the following: i) Two message sets (W_0, W_1) and (W_0, W_2) that are uniformly distributed over

¹This work was partially supported by Iran Telecom Research Center under contract no. 17175/500.

$[1 : M_0] \times [1 : M_1]$ and $[1 : M_0] \times [1 : M_2]$, respectively, where messages $W_u \in \mathcal{W}_u = \{1, 2, \dots, M_u\}$ and $u = 0, 1, 2$. Note that W_0 , W_1 and W_2 are independent. ii) A stochastic encoder f for transmitter 1 is specified by the matrix of conditional probability $f(X_1^n | w_0, w_1)$, where $X_1^n \in \mathcal{X}_1^n$, $w_0 \in \mathcal{W}_0$, $w_1 \in \mathcal{W}_1$ are channel input, common and private message sets respectively, and $\sum_{X_1^n} f(X_1^n | w_0, w_1) = 1$. Note that $f(X_1^n | w_0, w_1)$ is the probability of encoding message pair (w_0, w_1) to the channel input X_1^n . iii) A deterministic encoder g for transmitter 2 which is the mapping $g : \mathcal{W}_0 \times \mathcal{W}_2 \rightarrow \mathcal{X}_2^n$ for generating codewords $X_2^n = g(w_0, w_2)$. iv) A decoding function $\phi : \mathcal{Y}_1^n \rightarrow \mathcal{W}_0 \times \mathcal{W}_1 \times \mathcal{W}_2$ at the receiver 1 that assigns $(\widehat{W}_{01}, \widehat{W}_{11}, \widehat{W}_{21}) \in [1 : M_0] \times [1 : M_1] \times [1 : M_2]$ to received sequence y_1^n . v) A decoding function $\rho : \mathcal{Y}_2^n \rightarrow \mathcal{W}_0 \times \mathcal{W}_2$, at the receiver 2 that assigns $(\widehat{W}_{02}, \widehat{W}_{22}) \in [1 : M_0] \times [1 : M_2]$ to received sequence y_2^n . The probability of error is defined as,

$$P_e^n = \Pr(\widehat{W}_{0j} \neq W_0 \text{ for } j = 1, 2 \text{ or } \widehat{W}_{11} \neq W_1 \text{ or } \widehat{W}_{2j} \neq W_2 \text{ for } j = 1, 2). \quad (1)$$

The ignorance level of receiver 2 with respect to the confidential message is measured by the normalized equivocation $\frac{1}{n} H(W_1 | Y_2^n)$.

Definition 2: A rate tuple (R_0, R_1, R_2) is said to be achievable for CMAC-CM, if for any $\delta > 0$ there exists a $(M_0, M_1, M_2, n, P_e^n)$ code as

$$P_e^n < \varepsilon \quad (2)$$

$$M_0 \geq 2^{nR_0}, M_1 \geq 2^{nR_1}, M_2 \geq 2^{nR_2} \quad (3)$$

$$R_1 - \frac{1}{n} H(W_1 | Y_2^n) \leq \delta \quad (4)$$

III. MAIN RESULTS

A. Outer Bound

Theorem 1: (Outer bound) The secrecy capacity region for the CMAC-CM is included in the set of rates satisfying

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\} \quad (5)$$

$$R_1 \leq I(V_1; Y_1 | U, V_2) - I(V_1; Y_2 | U, V_2) \quad (6)$$

$$R_2 \leq \min\{I(V_2; Y_1), I(V_2; Y_2)\} \quad (7)$$

$$R_1 + R_2 \leq I(V_1, V_2; Y_1) - I(V_1; Y_2 | U, V_2) \quad (8)$$

for some joint distribution

$$p(u)p(v_1, v_2 | u)p(x_1 | v_1)p(x_2 | v_2)p(y_1, y_2 | x_1, x_2). \quad (9)$$

Remark 1: If we set $W_2 = \emptyset$ and thus $R_2 = 0$ in Theorem 1, the region reduces to the region of the broadcast channel with confidential messages discussed in [2] by Csiszár and Körner.

Proof (Theorem 1): We next show that any achievable rate tuples satisfies (5)-(8) for some distribution factorized as (9). Consider a code $(M_0, M_1, M_2, n, P_e^n)$ for the CMAC-CM. Applying Fano's inequality [11] results in

$$H(W_0, W_1, W_2 | Y_1^n) \leq n\varepsilon_1 \quad (10)$$

$$H(W_0, W_2 | Y_2^n) \leq n\varepsilon_2 \quad (11)$$

We first derive the bound on R_1 . Note that the perfect secrecy (4) implies that

$$nR_1 - n\delta \leq H(W_1 | Y_2^n). \quad (12)$$

Hence, we derive the bound on $H(W_1 | Y_2^n)$ as following:

$$\begin{aligned} H(W_1 | Y_2^n) &= H(W_1 | Y_2^n, W_0, W_2) + I(W_1; W_0, W_2 | Y_2^n) \\ &= H(W_1 | Y_2^n, W_0, W_2) + H(W_0, W_2 | Y_2^n) \\ &\quad - H(W_0, W_2 | Y_2^n, W_1) \\ &\leq H(W_1 | Y_2^n, W_0, W_2) + n\varepsilon_2 \\ &\leq H(W_1 | Y_2^n, W_0, W_2) - H(W_1 | Y_1^n, W_0, W_2) \\ &\quad + n\varepsilon_1 + n\varepsilon_2 \end{aligned} \quad (13)$$

where the first and the second inequality are due to Fano's inequalities. Now, based on (13) we have

$$\begin{aligned} H(W_1 | Y_2^n) &\leq I(W_1; Y_1^n | W_0, W_2) \\ &\quad - I(W_1; Y_2^n | W_0, W_2) + n\varepsilon \\ &= \sum_{i=1}^n [I(W_1; Y_{1,i} | Y_1^{i-1}, W_0, W_2) \\ &\quad - I(W_1; Y_{2,i} | Y_{2,i+1}^n, W_0, W_2)] + n\varepsilon \\ &= \sum_{i=1}^n [I(W_1; Y_{2,i+1}^n; Y_{1,i} | Y_1^{i-1}, W_0, W_2) \\ &\quad - I(Y_{2,i+1}^n; Y_{1,i} | Y_1^{i-1}, W_0, W_1, W_2) \\ &\quad - I(W_1, Y_1^{i-1}; Y_{2,i} | Y_{2,i+1}^n, W_0, W_2) \\ &\quad + I(Y_1^{i-1}; Y_{2,i} | Y_{2,i+1}^n, W_0, W_1, W_2)] + n\varepsilon \\ &= \sum_{i=1}^n [I(Y_{2,i+1}^n; Y_{1,i} | Y_1^{i-1}, W_0, W_2) \\ &\quad + I(W_1; Y_{1,i} | Y_{2,i+1}^n, Y_1^{i-1}, W_0, W_2) \\ &\quad - I(Y_{2,i+1}^n; Y_{1,i} | Y_1^{i-1}, W_0, W_1, W_2) \\ &\quad - I(Y_1^{i-1}; Y_{2,i} | Y_{2,i+1}^n, W_0, W_2) \\ &\quad - I(W_1; Y_{2,i} | Y_{2,i+1}^n, Y_1^{i-1}, W_0, W_2) \\ &\quad + I(Y_1^{i-1}; Y_{2,i} | Y_{2,i+1}^n, W_0, W_1, W_2)] + n\varepsilon \\ &= \sum_{i=1}^n [I(W_1; Y_{1,i} | Y_{2,i+1}^n, Y_1^{i-1}, W_0, W_2) \\ &\quad - I(W_1; Y_{2,i} | Y_{2,i+1}^n, Y_1^{i-1}, W_0, W_2)] + n\varepsilon \end{aligned}$$

where $\varepsilon = \varepsilon_1 + \varepsilon_2$. The last equality is due to [2, Lemma 7] where:

$$\begin{aligned} \sum_{i=1}^n I(Y_{2,i+1}^n; Y_{1,i} | Y_1^{i-1}, W_0, W_2) &= \\ \sum_{i=1}^n I(Y_1^{i-1}; Y_{2,i} | Y_{2,i+1}^n, W_0, W_2) \end{aligned} \quad (14)$$

and

$$\begin{aligned} \sum_{i=1}^n I(Y_{2,i+1}^n; Y_{1,i} | Y_1^{i-1}, W_0, W_1, W_2) &= \\ \sum_{i=1}^n I(Y_1^{i-1}; Y_{2,i} | Y_{2,i+1}^n, W_0, W_1, W_2). \end{aligned} \quad (15)$$

So, we have

$$\begin{aligned} H(W_1 | Y_2^n) &\leq \sum_{i=1}^n [I(W_1; Y_{1,i} | U_i, V_{2,i}) \\ &\quad - I(W_1; Y_{2,i} | U_i, V_{2,i})] + n\varepsilon \\ &= \sum_{i=1}^n [I(V_{1,i}; Y_{1,i} | U_i, V_{2,i}) - I(V_{1,i}; Y_{2,i} | U_i, V_{2,i})] + n\varepsilon \end{aligned} \quad (16)$$

where the equalities resulting from the following definitions of the random variables

$$U_i = Y_{2,i+1}^n, Y_1^{i-1}, W_0 \quad (17)$$

$$V_{1,i} = (U_i, W_1) \quad (18)$$

$$V_{2,i} = (U_i, W_2). \quad (19)$$

Now, we have

$$\begin{aligned} H(W_1|Y_2^n) &\leq n \sum_{i=1}^n \frac{1}{n} [I(V_{1,Q}; Y_{1,Q}|U_Q, V_{2,Q}, Q=i) \\ &\quad - I(V_{1,Q}; Y_{2,Q}|U_Q, V_{2,Q}, Q=i)] + n\varepsilon \\ &= n \sum_{i=1}^n p(Q=i) [I(V_{1,Q}; Y_{1,Q}|U_Q, V_{2,Q}, Q=i) \\ &\quad - I(V_{1,Q}; Y_{2,Q}|U_Q, V_{2,Q}, Q=i)] + n\varepsilon \\ &= n [I(V_{1,Q}; Y_{1,Q}|U_Q, V_{2,Q}, Q) \\ &\quad - I(V_{1,Q}; Y_{2,Q}|U_Q, V_{2,Q}, Q)] + n\varepsilon \\ &= n [I(V_1; Y_1|U, V_2) - I(V_1; Y_2|U, V_2)] + n\varepsilon \quad (20) \end{aligned}$$

where $V_{1,Q} = V_1$, $V_{2,Q} = V_2$, $Y_{1,Q} = Y_1$, $Y_{2,Q} = Y_2$, $(U_Q, Q) = U$ and Q has a uniform distribution over $\{1, 2, \dots, n\}$ outcomes. Now, we derive the bound on R_2 as following:

$$\begin{aligned} nR_2 &= H(W_2) = H(W_2|W_0) \\ &= I(W_2; Y_1^n|W_0) + H(W_2|Y_1^n, W_0) \\ &\leq I(W_2; Y_1^n|W_0) + n\varepsilon_1 \quad (21) \end{aligned}$$

where the second equality results from independence of W_0, W_1, W_2 , and the inequality is due to the Fano's inequality. Now, based on (21)

$$\begin{aligned} nR_2 &\leq \sum_{i=1}^n I(W_2; Y_{1,i}|Y_1^{i-1}, W_0) + n\varepsilon_1 \\ &\leq \sum_{i=1}^n I(W_2, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_0) + n\varepsilon_1 \\ &\leq \sum_{i=1}^n I(W_2, W_0, Y_{2,i+1}^n, Y_1^{i-1}; Y_{1,i}) + n\varepsilon_1 \\ &= \sum_{i=1}^n I(V_{2,i}, U_i; Y_{1,i}) + n\varepsilon_1 \quad (22) \end{aligned}$$

where the last equality follows from (17) and (19). Now, we have

$$\begin{aligned} R_2 &\leq \sum_{i=1}^n \frac{1}{n} [I(V_{2,i}, U_i; Y_{1,i})] + n\varepsilon_1 \\ &= \sum_{i=1}^n \frac{1}{n} [I(V_{2,Q}, U_Q; Y_{1,Q}|Q=i)] + n\varepsilon_1 \\ &= \sum_{i=1}^n p(Q=i) [I(V_{2,Q}, U_Q; Y_{1,Q}|Q=i)] + n\varepsilon_1 \\ &= I(V_{2,Q}, U_Q; Y_{1,Q}|Q) + n\varepsilon_1 \\ &= I(V_{2,Q}, U_Q, Q; Y_{1,Q}) + n\varepsilon_1 \\ &= I(V_{2,Q}; Y_{1,Q}) + I(U_Q; Y_{1,Q}|V_{2,Q}) \\ &\quad + I(Q; Y_{1,Q}|V_{2,Q}, U_Q) + n\varepsilon_1 \\ &= I(V_{2,Q}; Y_{1,Q}) + n\varepsilon_1 \\ &= I(V_2; Y_1) + n\varepsilon_1 \quad (23) \end{aligned}$$

where fourth equality result from independence of Q and Y_Q . Sixth equality is due to $I(U_Q; Y_{1,Q}|V_{2,Q}) = 0$ (see (17) and (19)), and $I(Q; Y_{1,Q}|V_{2,Q}, U_Q) = 0$ since Q is independent of

$Y_{1,Q}$. The last equality results by setting $V_{2,Q} = V_2$, $Y_{1,Q} = Y_1$.

On the other hand, we have:

$$\begin{aligned} nR_2 &= H(W_2) = H(W_2|W_0) \\ &= I(W_2; Y_2^n|W_0) + H(W_2|Y_2^n, W_0) \\ &\leq I(W_2; Y_2^n|W_0) + n\varepsilon_2 \quad (24) \end{aligned}$$

where the inequality is due to the Fano's inequality. Next, we have

$$\begin{aligned} nR_2 &\leq \sum_{i=1}^n I(W_2; Y_{2,i}|Y_{2,i+1}^n, W_0) + n\varepsilon_2 \\ &\leq \sum_{i=1}^n I(W_2, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_0) + n\varepsilon_2 \\ &\leq \sum_{i=1}^n I(W_2, Y_{2,i+1}^n, Y_1^{i-1}, W_0; Y_{2,i}) + n\varepsilon_2 \\ &= \sum_{i=1}^n I(U_i, V_{2,i}; Y_{2,i}) + n\varepsilon_2 \quad (25) \end{aligned}$$

where the last equality follows from (17) and (19). Now, by applying the same time-sharing strategy as (23) we have

$$R_2 \leq I(V_2; Y_2). \quad (26)$$

Now, we derive the bound on $n(R_1 + R_2)$ as following:

$$\begin{aligned} n(R_1 + R_2) &= H(W_1, W_2) = H(W_1, W_2|W_0) \\ &= I(W_1, W_2; Y_1^n|W_0) + H(W_1, W_2|Y_1^n, W_0) \\ &\leq I(W_1, W_2; Y_1^n|W_0) + n\varepsilon_1 \end{aligned}$$

where the inequality is due to the Fano's inequality. Now, we have

$$\begin{aligned} n(R_1 + R_2) &\leq I(W_1, W_2; Y_1^n|W_0) \\ &\quad - (H(W_1) - H(W_1|Y_2^n) - n\delta) + n\varepsilon_1 \\ &= I(W_1, W_2; Y_1^n|W_0) - H(W_1|W_0, W_2) \\ &\quad + H(W_1|Y_2^n) + n(\varepsilon_1 + \delta) \\ &= I(W_1, W_2; Y_1^n|W_0) - H(W_1|W_0, W_2) \\ &\quad + H(W_1|Y_2^n, W_0, W_2) \\ &\quad + I(W_1; W_0, W_2|Y_2^n) + n(\varepsilon_1 + \delta) \\ &\leq I(W_1, W_2; Y_1^n|W_0) \\ &\quad - I(W_1; Y_2^n|W_0, W_2) + n\varepsilon_2 + n(\varepsilon_1 + \delta) \end{aligned}$$

where the first inequality is a consequence of (4) and the last inequality is due to the Fano's inequality. We also define $\varepsilon_3 = \varepsilon_1 + \varepsilon_2 + \delta$. So, we have

$$\begin{aligned} n(R_1 + R_2) &\leq \sum_{i=1}^n [I(W_1, W_2; Y_{1,i}|Y_1^{i-1}, W_0) \\ &\quad - I(W_1; Y_{2,i}|Y_{2,i+1}^n, W_0, W_2)] + n\varepsilon_3 \\ &= \sum_{i=1}^n [I(W_1, W_2, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_0) \\ &\quad - I(Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_0, W_1, W_2) \\ &\quad - I(W_1, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_0, W_2) \\ &\quad + I(Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_0, W_1, W_2)] + n\varepsilon_3 \\ &= \sum_{i=1}^n [I(W_1, W_2, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_0) \\ &\quad - I(W_1, Y_1^{i-1}; Y_{2,i}|Y_{2,i+1}^n, W_0, W_2)] + n\varepsilon_3 \end{aligned}$$

where the last equality is a consequence of (15). Hence, we have

$$\begin{aligned} n(R_1 + R_2) &\leq \sum_{i=1}^n [I(W_1, W_2, Y_{2,i+1}^n; Y_{1,i}|Y_1^{i-1}, W_0) \\ &\quad - I(W_1; Y_{2,i}|Y_{2,i+1}^n, Y_1^{i-1}, W_0, W_2)] + n\varepsilon_3 \\ &\leq \sum_{i=1}^n [I(W_0, W_1, W_2, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1,i}) \\ &\quad - I(W_1; Y_{2,i}|Y_{2,i+1}^n, Y_1^{i-1}, W_0, W_2)] + n\varepsilon_3. \end{aligned}$$

Now, we have

$$\begin{aligned} n(R_1 + R_2) &\leq \sum_{i=1}^n [I(U_i, V_{1,i}, V_{2,i}; Y_{1,i}) \\ &\quad - I(V_{1,i}; Y_{2,i}|U_i, V_{2,i})] + n\varepsilon_3 \end{aligned}$$

where the inequality follows from (17)-(19). Now, by applying the same time-sharing strategy as before, we have:

$$R_1 + R_2 \leq I(V_1, V_2; Y_1) - I(V_1; Y_2|U, V_2). \quad (27)$$

Now, we derive the bound on R_0 as following:

$$\begin{aligned} nR_0 &= H(W_0) = I(W_0; Y_1^n) + H(W_0|Y_1^n) \\ &\leq I(W_0; Y_1^n) + n\varepsilon_1 \\ &= \sum_{i=1}^n I(W_0; Y_{1,i}|Y_1^{i-1}) + n\varepsilon_1 \\ &= \sum_{i=1}^n [I(W_0, Y_1^{i-1}; Y_{1,i}) - I(Y_1^{i-1}; Y_{1,i})] + n\varepsilon_1. \end{aligned}$$

So, we have

$$\begin{aligned} nR_0 &\leq \sum_{i=1}^n I(W_0, Y_1^{i-1}; Y_{1,i}) + n\varepsilon_1 \\ &\leq \sum_{i=1}^n [I(W_0, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1,i}) \\ &\quad - I(Y_{2,i+1}^n; Y_{1,i}|W_0, Y_1^{i-1})] + n\varepsilon_1 \\ &\leq \sum_{i=1}^n I(W_0, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1,i}) + n\varepsilon_1 \\ &= \sum_{i=1}^n I(U_i; Y_{1,i}) + n\varepsilon_1. \end{aligned}$$

Now, by applying the same time-sharing strategy as before, we have

$$R_0 \leq I(U; Y_1) + \varepsilon_1. \quad (28)$$

Similarly

$$R_0 \leq I(U; Y_2) + \varepsilon_2. \quad (29)$$

Therefore

$$R_0 \leq \min\{I(U; Y_1), I(U; Y_2)\}. \quad (30)$$

Considering (12), (20), (23), (26), (27) and (30), the region in (5)-(8) is obtained. This completes the proof. ■

B. Achievability

Theorem 2: An inner bound on the secrecy capacity region is given by:

$$\bigcup \left\{ \begin{array}{l} R_0 \geq 0, R_1 \geq 0, R_2 \geq 0 \\ R_1 \leq I(V_1; Y_1|X_2, U) - I(V_1; Y_2|X_2, U) \\ R_2 \leq \min\{I(X_2; Y_1|V_1, U), I(X_2; Y_2|U)\} \\ R_0 + R_2 \leq I(U, X_2; Y_2) \\ R_1 + R_2 \leq I(V_1, X_2; Y_1|U) - I(V_1; Y_2|X_2, U) \\ R_0 + R_1 + R_2 \leq I(V_1, X_2; Y_1) - I(V_1; Y_2|X_2, U) \end{array} \right. \quad (31)$$

where the union is taken over all probability distributions of the form $p(u, v_1, x_1, x_2, y_1, y_2) = p(u)p(v_1|u)p(x_1|v_1)p(x_2|u)p(y_1, y_2|x_1, x_2)$.

Remark 2: If we convert our model to a multiple access channel with correlated sources by setting $Y_2 = \emptyset$ and $V_1 = X_1$ in Theorem 2, the region reduces to the region of the multiple access channel with correlated sources discussed in [12] by Slepian and Wolf.

Remark 3: If we set $X_2 = \emptyset$ in Theorem 2, the region includes the region of the broadcast channel with confidential messages discussed in [2] by Csiszár and Körner.

Proof (Theorem 2): Fix $p(u), p(v_1|u), p(x_1|v_1)$ and $p(x_2|u)$.

1) *Codebook generation:*

- i) Generate 2^{nR_0} codewords u^n , each is uniformly drawn from the set $A_\varepsilon^n(P_U)$ indexing by $u^n(w_0)$, $w_0 \in \{1, \dots, 2^{nR_0}\}$.
- ii) For each codeword $u^n(w_0)$, generate $2^{n\tilde{R}}$ codewords v_1^n each is uniformly drawn from the set $A_\varepsilon^n(P_{V_1|U})$, where $\tilde{R} = R_1 + I(V_1; Y_2|X_2, U) - \varepsilon$. Then, randomly bin the $2^{n\tilde{R}}$ codewords into 2^{nR_1} bins and label them as $v_1^n(w_0, w_1, l)$. Here, w_1 is the bin number and $l \in \mathcal{L} = \{1, \dots, 2^{n(I(V_1; Y_2|X_2, U) - \varepsilon)}\}$ is the index of codewords in the bin number w_1 .
- iii) For each codeword $u^n(w_0)$, generate 2^{nR_2} codewords $x_2^n(w_0, w_2)$ each is uniformly drawn from the set $A_\varepsilon^n(P_{X_2|U})$, and label them as $x_2^n(w_0, w_2)$, $w_2 \in \{1, \dots, 2^{nR_2}\}$.

2) *Encoding:* To send the message pair (w_0, w_1) , the encoder f first randomly chooses index l corresponding to (w_0, w_1) and then, generates a codeword X_1^n at random according to $\prod_{i=1}^n p(x_{1,i}|v_{1,i})$. Transmitter 2 uses the deterministic encoder for sending (w_0, w_2) and sends codeword $x_2^n(w_0, w_2)$.

3) *Decoding and Probability of error:*

- Receiver 1 declares that the indices of $(\hat{w}_{01}, \hat{w}_{11}, \hat{w}_{21})$ has been sent if there is a unique tuple of indices $(\hat{w}_{01}, \hat{w}_{11}, \hat{w}_{21})$ such that $(u^n(\hat{w}_{01}), v_1^n(\hat{w}_{01}, \hat{w}_{11}, l), x_2^n(\hat{w}_{01}, \hat{w}_{21}), y_1^n) \in A_\varepsilon^n(P_{UV_1X_2Y_1})$.
- Receiver 2 declares that the index pair of $(\hat{w}_{02}, \hat{w}_{22})$ has been sent if there is a unique pair of indices $(\hat{w}_{02}, \hat{w}_{22})$ such that $(u^n(\hat{w}_{02}), x_2^n(\hat{w}_{02}, \hat{w}_{22}), y_2^n) \in A_\varepsilon^n(P_{UX_2Y_2})$.

Using joint decoding [11], it can be shown that the probability of error goes to zero as $n \rightarrow \infty$ if we choose:

$$R_1 \leq I(V_1; Y_1|X_2, U) - I(V_1; Y_2|X_2, U) \quad (32)$$

$$R_2 \leq \min\{I(X_2; Y_1|V_1, U), I(X_2; Y_2|U)\} \quad (33)$$

$$R_0 + R_2 \leq I(U, X_2; Y_2) \quad (34)$$

$$R_1 + R_2 \leq I(V_1, X_2; Y_1|U) - I(V_1; Y_2|X_2, U) \quad (35)$$

$$R_0 + R_1 + R_2 \leq I(U, V_1, X_2; Y_1) - I(V_1; Y_2|X_2, U) \quad (36)$$

4) Equivocation computation:

$$\begin{aligned}
H(W_1|Y_2^n) &\geq H(W_1|Y_2^n, X_2^n, U^n) \\
&= H(W_1, Y_2^n|X_2^n, U^n) - H(Y_2^n|X_2^n, U^n) \\
&= H(W_1, Y_2^n, V_1^n|X_2^n, U^n) \\
&\quad - H(V_1^n|W_1, Y_2^n, X_2^n, U^n) - H(Y_2^n|X_2^n, U^n) \\
&= H(W_1, V_1^n|X_2^n, U^n) \\
&\quad + H(Y_2^n|W_1, V_1^n, X_2^n, U^n) \\
&\quad - H(V_1^n|W_1, Y_2^n, X_2^n, U^n) - H(Y_2^n|X_2^n, U^n) \\
&\geq H(V_1^n|X_2^n, U^n) + H(Y_2^n|V_1^n, X_2^n, U^n) \\
&\quad - H(V_1^n|W_1, Y_2^n, X_2^n, U^n) - H(Y_2^n|X_2^n, U^n) \\
&= H(V_1^n|U^n) - H(V_1^n|W_1, Y_2^n, X_2^n, U^n) \\
&\quad - I(V_1^n; Y_2^n|X_2^n, U^n)
\end{aligned} \tag{37}$$

where the last inequality is due to the fact that V_1^n is a function of W_1 and the last equality follows from the Markov chain $V_1^n - U^n - X_2^n$. The first term in (37) is given by:

$$H(V_1^n|U^n) = n\tilde{R}. \tag{38}$$

We then show that $H(V_1^n|W_1, Y_2^n, X_2^n, U^n) \leq n\varepsilon_1$, where as $n \rightarrow \infty$ then $\varepsilon_1 \rightarrow 0$. Based on the Fano's inequality, we have:

$$H(V_1^n|W_1 = w_1, Y_2^n, X_2^n, U^n) \leq 1 + p_{ew_1}(n\tilde{R} - nR_1) \equiv n\varepsilon_1$$

where p_{ew_1} specifies the average of error probability of user 1 for decoding $v_1^n(w_0, w_1, l)$ given $W_1 = w_1$ and $W_0 = w_0$. Hence

$$\begin{aligned}
H(V_1^n|W_1, Y_2^n, X_2^n, U^n) &= \\
\sum_{w_1 \in \mathcal{W}_1} p(W_1 = w_1) H(V_1^n|W_1 = w_1, Y_2^n, X_2^n, U^n) &\leq n\varepsilon_1.
\end{aligned} \tag{39}$$

The last term in (37) is bounded as:

$$I(V_1^n; Y_2^n|X_2^n, U^n) \leq nI(V_1; Y_2|X_2, U) + n\varepsilon_2 \tag{40}$$

where as $n \rightarrow \infty$, then $\varepsilon_2 \rightarrow 0$ [1, Lemma 8]. By replacing (38)-(40) in equation (37), and setting $\delta = \varepsilon_1 + \varepsilon_2$, we have:

$$\begin{aligned}
H(W_1|Y_2^n) &\geq n\tilde{R} - n\varepsilon_1 - nI(V_1; Y_2|X_2, U) - n\varepsilon_2 \\
&= n(\tilde{R} - I(V_1; Y_2|X_2, U)) - n\delta \\
&= nR_1 - n\delta.
\end{aligned} \tag{41}$$

This completes the proof of Theorem 2. ■

IV. EXAMPLES

In this section, we consider less noisy and Gaussian CMAC-CM.

A. Less Noisy CMAC-CM

We define 'less noisy' model as a CMAC-CM where $I(V_2; Y_1) \geq I(V_2; Y_2)$ for all $p(v_2, x_2)$.

Theorem 3 (Outer Bound): The secrecy capacity region for the less noisy CMAC-CM is included in the set of rates satisfying

$$R_1 \leq I(V_1; Y_1|V_2) - I(V_1; Y_2|V_2) \tag{42}$$

$$R_2 \leq I(V_2; Y_2) \tag{43}$$

$$R_1 + R_2 \leq I(V_1, V_2; Y_1) - I(V_1; Y_2|V_2) \tag{44}$$

for some joint distribution

$$p(v_1, v_2)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2).$$

Proof: The proof is similar to Theorem 1. If we set $R_0 = 0$ and define $V_{1,i} = (Y_{2,i+1}^n, Y_1^{i-1}, W_1)$ and $V_{2,i} = (Y_{2,i+1}^n, Y_1^{i-1}, W_2)$, we can derive (42) to (44). ■

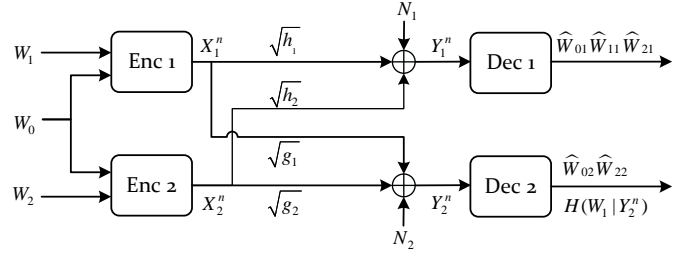


Fig. 2 Gaussian compound MAC with confidential messages.

Theorem 4 (Achievability): An inner bound on the secrecy capacity region is given by:

$$\bigcup \left\{ \begin{aligned} R_1 &\leq I(V_1; Y_1|V_2) - I(V_1; Y_2|V_2) \\ R_2 &\leq I(V_2; Y_2) \\ R_1 + R_2 &\leq I(V_1, V_2; Y_1) - I(V_1; Y_2|V_2) \end{aligned} \right. \tag{45}$$

where the union is taken over all joint distributions factorized as $p(v_1)p(v_2)p(x_1|v_1)p(x_2|v_2)p(y_1, y_2|x_1, x_2)$.

Proof: The proof follows from Theorem 2 by setting U as a constant and by replacing X_2 by V_2 where V_2 is obtained by passing X_2 through a DMC $p(v_2|x_2)$. Note that

$$\begin{aligned}
I(V_2; Y_1|V_1) &= H(V_2|V_1) - H(V_2|Y_1, V_1) \\
&\stackrel{(a)}{=} H(V_2) - H(V_2|Y_1, V_1) = I(V_2; Y_1, V_1) \\
&\geq I(V_2; Y_1) \stackrel{(b)}{\geq} I(V_2; Y_2)
\end{aligned}$$

where (a) happens since V_1 and V_2 are independent and (b) results from considering less noisy model. Therefore, we have $\min\{I(V_2; Y_1|V_1), I(V_2; Y_2)\} = I(V_2; Y_2)$. ■

Note that although the outer and inner bounds for this model has the same characteristic, they are over two different joint distributions.

B. Gaussian CMAC-CM

In this section, we consider Gaussian CMAC-CM as depicted in Fig. 2, and extend the achievable rate region of discrete memoryless CMAC-CM to the Gaussian case. Relationships between the inputs and outputs of the channel are given by

$$Y_1 = \sqrt{h_1}X_1 + \sqrt{h_2}X_2 + N_1 \tag{46}$$

$$Y_2 = \sqrt{g_1}X_1 + \sqrt{g_2}X_2 + N_2 \tag{47}$$

where h_i, g_i (for $i = 1, 2$) are known channel gains as shown in Fig. 2. The noise terms N_1 and N_2 are independent zero-mean unit-variance complex Gaussian random variables and independent of the real random variables X_1, X_2 . The inputs of the channel are also subject to an average power constraint

$$\frac{1}{n} \sum_{i=1}^n E[X_{k,i}^2] \leq P_k \quad k = 1, 2. \tag{48}$$

Let V_1, V_2, X_1 , and X_2 be jointly Gaussian random variables with

$$V_1 = \sqrt{P_{U_1}}U + \sqrt{P_{U'}}U', \quad V_2 = \sqrt{P_{U_2}}U + \sqrt{P_{U''}}U'' \tag{49}$$

$$V_1 \triangleq X_1, \quad V_2 \triangleq X_2 \tag{50}$$

where U, U' and U'' are independent Gaussian zero mean unit variance random variables. The terms $P_{U_1}, P_{U_2}, P_{U'}$, and $P_{U''}$ denote the corresponding power allocation, where

$$P_1 = P_{U_1} + P_{U'}, \quad P_2 = P_{U_2} + P_{U''}. \tag{51}$$

Following the achievability proof for the discrete memoryless channel, we obtain the following result for the Gaussian CMAC-CM.

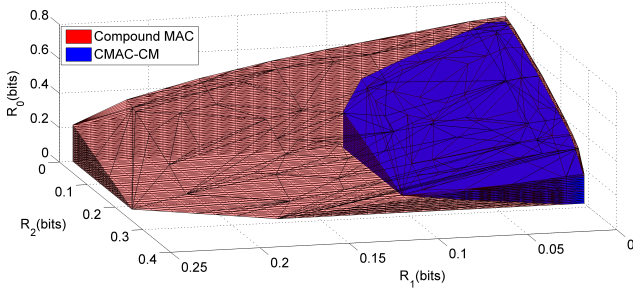


Fig. 3 Achievable rate region of Gaussian CMAC-CM and the capacity region of Compound MAC for $P_1 = P_2 = 1$, $h_1 = h_2 = 0.6$, $g_1 = 0.4$ and $g_2 = 0.5$.

Theorem 5: An inner bound on the secrecy capacity region of Gaussian CMAC-CM is:

$$\bigcup \left\{ \begin{array}{l} R_1 \leq C(h_1 P_{U'}) - C(g_1 P_{U'}) \\ R_2 \leq \min\{C(h_2 P_{U''}), C(\frac{g_2 P_{U''}}{1+g_1 P_{U'}})\} \\ R_0 + R_2 \leq C(\frac{g_1 P_{U_1} + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U_1} P_{U_2}}}{1+g_1 P_{U'}}) \\ R_1 + R_2 \leq C(h_1 P_{U'} + h_2 P_{U''}) - C(g_1 P_{U'}) \\ R_0 + R_1 + R_2 \leq C(h_1 P_1 + h_2 P_2 + 2\sqrt{h_1 h_2 P_{U_1} P_{U_2}}) - C(g_1 P_{U'}) \end{array} \right. \quad (52)$$

where $C(x) = (1/2)\log(1+x)$ and the union is taken over all $0 \leq P_{U_1} + P_{U'} \leq P_1$ and $0 \leq P_{U_2} + P_{U''} \leq P_2$.

Proof: Following from Theorem 2, by choosing random variables the same as (46)-(51) the region in (52) is derived.

Theorem 6: The capacity region of Compound Gaussian MAC is given by:

$$\bigcup \left\{ \begin{array}{l} 0 \leq R_1 \leq \min\{C(h_1 P_{U'}), C(g_1 P_{U'})\} \\ 0 \leq R_2 \leq \min\{C(h_2 P_{U''}), C(g_2 P_{U''})\} \\ 0 \leq R_1 + R_2 \leq \min\{C(h_1 P_{U'} + h_2 P_{U''}), C(g_1 P_{U'} + g_2 P_{U''})\} \\ 0 \leq R_0 + R_1 + R_2 \leq \min\{C(h_1 P_1 + h_2 P_2 + 2\sqrt{h_1 h_2 P_{U_1} P_{U_2}}), C(g_1 P_1 + g_2 P_2 + 2\sqrt{g_1 g_2 P_{U_1} P_{U_2}})\} \end{array} \right. \quad (53)$$

where $C(x) = (1/2)\log(1+x)$ and the union is taken over all $0 \leq P_{U_1} + P_{U'} \leq P_1$ and $0 \leq P_{U_2} + P_{U''} \leq P_2$.

Proof: Considering Propositions 6.1 and 6.2 in [10] which are outer and inner bounds on the capacity region of compound MAC with conferencing links, then ignoring conferencing links in that model (i.e., setting $C_{12} = C_{21} = 0$ in [10]), and by considering (46) to (51), the region in (53) is derived. ■

As an example, for the values $P_1 = P_2 = 1$, $h_1 = h_2 = .6$, $g_1 = .4$ and $g_2 = .5$ the achievable rate region in Theorem 5 and the capacity region in Theorem 6 are depicted in Fig. 3. As it can be seen in Fig. 3, for this scenario the achievable rate R_0 (rate of W_0 which is decoded by both receivers) is nearly the same for both CMAC-CM and compound MAC models. Moreover, the achievable rate R_2 (rate of W_2 which is also decoded by both receivers) is equal for both CMAC-CM and compound MAC models. Moreover, as it can be seen from Fig. 3, for these channel gain parameters the achievable rate R_1 for CMAC-CM is less than that for Compound MAC due to secrecy constraint for decoding message W_1 .

According to (53), it is clear that if the channel gain between transmitter 1 and receiver 2 (i.e., g_1) decreases, the capacity region of compound MAC does not increase (i.e., the capacity region may remain as before or decreases). On the other hand, there exist scenarios for CMAC-CM (refer to (52)) for which decreasing g_1 results in increasing its achievable rate region. For comparison, assume changing $g_1 = 0.4$ to $g_1 = 0.1$ in the above example. As it can be seen in Fig. 4, the achievable rate region of CMAC-CM is larger than the capacity region of compound MAC model for the new parameters. This can be interpreted as follows: transmitted signal of

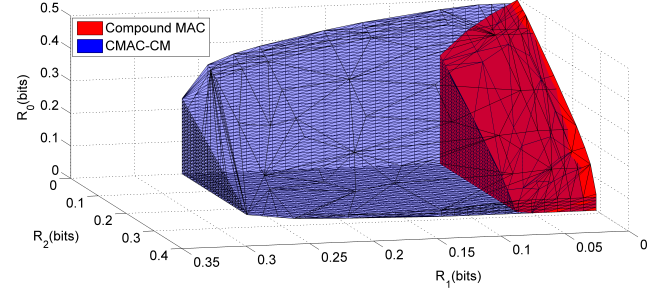


Fig. 4 Achievable rate region of Gaussian CMAC-CM and the capacity region of Compound MAC for $P_1 = P_2 = 1$, $h_1 = h_2 = 0.6$, $g_1 = 0.1$ and $g_2 = 0.5$.

transmitter 1 is extremely attenuated at the receiver 2. So, for this case, not forcing the receiver 2 to decode W_1 (keeping W_1 as a secret for receiver 2) can increase the achievable rate region.

Also, it should be noted that according to (52), for the scenarios where g_1 equals or greater than h_1 , the achievable rate R_1 is zero. This happens since for these scenarios the channel gain between transmitter 1 and receiver 2 (i.e., illegal user in terms of message W_1) is equal or better than the channel gain between transmitter 1 and receiver 1 (i.e., legitimate user in terms of message W_1), and this makes zero R_1 .

V. CONCLUSIONS

In this paper, we have studied the secrecy capacity region of the Compound MAC with one Confidential Message (CMAC-CM). We have obtained inner and outer bounds on the secrecy capacity for the general CMAC-CM. We have further studied less noisy and Gaussian CMAC-CM. Providing numerical examples for the Gaussian case we have shown that there are scenarios for which keeping secret some messages can increase the rate region compared to being required to communicate those messages reliably to the other receiver.

REFERENCES

- [1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 57, no. 8, p. 13551367, Oct 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [3] X. Tang, R. Liu, P. Spasojević, and H. V. Poor, "Multiple access channels with generalized feedback and confidential messages," in *Proc. IEEE Info. Theory Workshop (ITW)*, CA, USA, Sep 2007, pp. 608–613.
- [4] L. Liang and H. V. Poor, "Multiple-access channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 3, no. 3, pp. 976–1002, Mar 2008.
- [5] E. Ekrem and S. Ulukus, "On the secrecy of multiple access wiretap channel," in *Proc. 46th Annual Allerton Conference on Communication, Control, and Computing*, Monticello, IL, Sep 2008, pp. 1014–1021.
- [6] M. Yassaee and M. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. IEEE Info. Theory Workshop (ITW)*, Dublin, Ireland, Sep 2010, pp. 1–5.
- [7] M. Wiese and H. Boche, "An achievable region for the wiretap multiple-access channel with common message," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Cambridge, MA, Jul 2012, pp. 249–253.
- [8] R. Liu, I. Marić, R. D. Yates, and P. Spasojević, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. on Info. Theory (ISIT)*, Seattle, WA, Sep 2006, pp. 957–961.
- [9] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*, 1st ed. Hanover, MA, USA: Now Publishers Inc., 2009.
- [10] O. Simeone, D. Gündüz, H. V. Poor, A. J. Goldsmith, and S. Shamai, "Compound multiple-access channels with partial cooperation," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2425–2441, Jun 2009.
- [11] A. El Gamal and Y. H-Kim, *Network information theory*, 1st ed. Cambridge, U.K: Cambridge University Press, 2012.
- [12] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell System Technical Journal*, vol. 52, no. 7, pp. 1037–1076, Sep 1973.